A Survey on Protection against Power Depletion Attack in WSN

Sruthin R.V. #1, Jayasudha J. S. #2

[1]M.Tech Student [2]HOD,
[#] Dept. of CSE, SCTCE, Pappanamcode, Trivandrum, India

Abstract— **Ad-hoc wireless sensor networks (WSNs) has large applications in present and future world. WSN is mainly used in areas where instant deployment of communication and computational resource is required. It is mainly used in areas like military war front, disastrous stood area, for researchers in remote places like deep forest and deserted places. The attackers are focusing on DoS attack in the networks. Permanent denial of service attack is performed by completely draining out the network nodes battery power. For preserving nodes battery power, reduce the cost of transmission and prevent the battery power draining attacks. There are many existing effective approaches for attack prevention. These approaches are compared to determine the finest of them. This review will help the researchers to do the future research.**

Keywords— ***WSN;*** **Energy Depletion Attack; Leashes; PLGPa**

I. Introduction

Ad-hoc wireless sensor networks (WSNs) has application in areas where no other communication and computational resource are available. The availability of network has a large impact. So attack is performed by completely depleting nodes battery power and making the network to dead state. This is different from short term DoS attack, reduction of quality (RoQ) attack, routing infrastructure attacks, since they disable the network for only short period of time. This attack is performed by unnecessarily making all the nodes in network active by simply making packets rome in the network. Let us consider a scenario, in which an attacker node creates packets in such a way that it rotates in network until it is time out. Many methods are used by attacker nodes to re-route the incoming packets, drops packets, change path of packets etc. thus more packets are roaming in network and energy is draining.

Energy saving in WSNs can be performed by two ways: The first method is to reduce the cost of transmission of packets. The second way is to prevent all the energy depletion attack and anomalies in the network. Many procedures and routing algorithms already exist to solve these issues. Some of the best methods and algorithms are analyzed here.

II. Transmission Cost

Transmission cost is the energy required to transmit a packet from one point to another. The packet is transmitted using radio signals.

A. An on-demand minimum energy routing protocol

Sheetalkumar Doshi et.al introduced the on-demand minimum energy routing protocol [1]. The energy required for radio transmission under ideal condition to a distance *r* is proportional to r^d where d is the range two to four. As the distance for transmission increases, the energy requirement also increases exponentially. Thus to reduce energy for transmission, the best method is to increase the intermediate node. For example, two nodes P and Q are 4 meter apart and they need 16 units of energy to transmit data from P to Q. If there is an intermediate node R such that it is 2 meter apart from both P and Q. Thus the energy required to transmit data from node P to Q through R is only 8 Units

Energy model used

The energy model helps us justify the required features of a minimum energy routing protocol. The energy expended in sending a data-packet of size D bytes over a given link can be modeled as equation 2.1 to 2.3.

$$E(D) = K_1 + K_2 \qquad (2.1)$$

$$K1 = (P_t^{packet} + P^{back}) / BR \qquad (2.2)$$

$$K_2 = ((P_t^{MAC} D^{MAC} + P_t^{packet} D^{header}) / BR) + E^{back} \qquad (2.3)$$

P^{back} and E^{back} are the background power and energy used in sending the data-packet, P_t^{MAC} is the power at which the MAC packet are transmitted, D^{MAC} is the size of the MAC packets in bytes, D^{header} is the size of the data-packet trailer and header, P_t^{packet} is the power at which the data-packet is transmitted and *BR* is the transmission rate in Bytes/sec. To simplify the analysis, assume P^{back} and E^{back} to be zero in the study.

Required energy decreases rapidly with distance

For a given threshold power P_r, the minimum transmit power P_t required for successful reception, assuming no fading, can be given as equation 2.4.

$$P_t(d) = P_r d^n / K \qquad (2.4)$$

where *d* is the distance between the two node, *n* is the path loss exponent and *K* is a constant. Typically *n* takes the value of 4. In case of maximum power minimum hope routing used in typical ad-hoc routing protocol like the current version of DSR, this transmit power is fixed to 280mW. Using equation (2.1), equation (2.2 and equation (2.3) the minimum transmission energy required for successful reception in terms of P_t and data-packet size *D* can be given as equation 2.5.

$$E_t(D,P_t) = k_1 P_t (D + D^{header}) + K_2 \qquad (2.5)$$

And substituting the value of P_t obtained from equation 2.4 in equation 2.5, we get equation 2.6.

$$E_t(D,d) = K_1^{''}(D + D^{header}) d^4 + K_2 \qquad (2.6)$$

Typical values for $K_1^{'}$, $K_1^{''}$ and K_2 in a two frame exchange 802.11 MAC environment with ACKs sent at full power and a 2MBps bit rate are 4*μs/byte,* 2.8 × 10^{-10} *μJ/(byte m*^{4}*)* and 42*μ* respectively. The transmission energy for the current version of the protocol (E_{max}) is fixed data-packet of size D bytes and can be given as equation 2.7.

$E_{max}(D) = K_3D = K_2$ (2.7)

where K_3 has the value of $1.162\mu/bytes$.

The energy that can be obtained by using the minimum transmits power instead of the fixed maximum power for the data-packet transmission is given as equation 2.8.

$S(D,d) = E_{max}(D) – E_t(D,d)$ (2.8)

Using multi-hop routes saves energy

Consider a case where the minimum hop routing protocol employs transmit power control. In this case there are 3 nodes a, b, c in a straight line and the minimum hop routing chooses to route data-packets directly from a to c. If the multi-hop route a-b-c is chosen to transmit the packets instead, i.e b is used as a relay node, the total transmit energy required would be

$E_{multi}(D,d,d_1) = E_t(D,d_1) + E_t(D,d - d_1)$

where d_1 is the distance from node a to node b and d is the distance from node a to node c.

The savings, $S(D,d,d_1)$, obtained by going the multihop route can be written as

$S(D,d,d_1) = E_t(D,d) - E_{multi}(D,d,d_1)$

i.e.

$S(D,d,d_1) = E_t(D,d) - E_t(D,d_1) - E_t(D,d - d_1)$

However the energy savings obtained by going multihop depends on the value of the fixed energy overhead K_2 and the distance from node a to node c.

Disadvantage of on-demand minimum energy routing protocol

On-demand minimum energy routing protocol is a method to reduce the transmission cost but the attackers can still make the packet rome in the network and drain the energy.

III. Preventing Energy Depletion Attack

A. All Packet Leashes

Packet Leashes is a defence mechanism against wormhole attacks in wireless ad hoc networks introduced by Yin Chun Hu, Adrian Perrig and David B. Johnson [2]. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them to another location and retransmits them there into the network [2]. The wormhole attack creates serious threats in many wireless routing protocols and location-based wireless security systems. Let as consider the example of neighbour discovery functionality in routing protocol OLSR [3], DSDV [6], and TBRPF [7]. Neighbour discovery function is performed by broadcasting of HELLO packets. If an attacker tunnels to A all the HELLO packets transmitted by B and vice versa. Then they will believe them as neighbours and the whole routing protocol will fail. Now if A and B are 2n+2 nodes apart, then n nodes closer to A cannot communicate to B and n nodes closer to B cannot communicate to A.

The method of packet leashes is used to defend these attacks. Any information that is added to a packet for restricting its movement to a maximum distance is called leash. Two types of leashes, geographical leashes and temporal leashes are introduces here. Geographical leashes ensure that the sender and receiver are within certain distance. Temporal leashes ensures that packets are active for only a certain time interval, so that packets will only travel a fixed distance since speed of packet is considered equal to speed of light.

Geographical Leashes

Geographical Leashes introduce limitations on the distance travelled by the packet from source to destination. Here each node has its own location information and the nodes have loosely synchronized clocks. The sending node sends the packet along with its location information q_s and the time at which the packet is sent, t_s. At the receiver side, the receiving node compare its location information q_r and the time at which the packet is received t_r with the that of the sender node. The clock of both sender and receiver is synchronized to within $\pm\Delta$ and v is the maximum velocity of any node. Now, the receiver can calculate the upper bound on the distance between sender and the receiver, d_{sr}. Specifically, based on the sending time t_s in the packet, the receive time t_r, the maximum relative error in location information δ and the locations of the sender q_s and the receiver q_r, then d_{sr} can be bounded by $d_{rs} \leq \| q_s – q_r \| + 2v(t_r – t_s + \Delta) + \delta$. A digital signature scheme is used for authenticating the location and timestamp in the received packet.

Temporal Leashes

In temporal leashes, all nodes must be tightly synchronized and the maximum allowable difference in time is Δ. In temporal leashes, the time at which the packet is sent, t_s are included in the sending packet. When the packet is received, the receiving node compares the sending time with the time at which it received the packet, t_r. Thus based on the transmission time and the speed of the light the receiver can verify the distance travelled by the packet. Thus the packet travelling more distance can be identified. Another method of constructing temporal leashes is to include in the packet an expiration time after which the packet is to be discarded. The expiration time is calculated on the basis of the maximum distance to be travelled and the time at which the packet is sent. Here also a digital signature scheme can be used to authenticate the time stamp or the expiration time in the packet.

Disadvantages of Packet Leashes

The main problem with packet leashes is that the nodes are to be tightly synchronised. Another problem with leashes using timestamp is that in a contention based MAC, the sender may not know the precise time at which the packet is send. For example, a sender using the IEEE 802.11 MAC may not know the time at which a packet will be transmitted until approximately one slot time prior to transmission.

B. Secure sensor network routing

Bryan et-al. proposed a clean-slate approach for assigning a network address to each node and establishes routing tables using a recursive grouping algorithm [4]. The routing of packets is then performed on the basis of the address table. The recursive grouping algorithm out puts a unique address to each node in network and the nodes in each sub group has similar prefix address. The address table created is used for effectively routing the packet through shortest distance path from source to destination.

Address and Routing Setup

At the initial stage every sensor node is considered as a group with size one. Then, the groups are repeatedly merged to form larger groups. The merging terminates when all nodes becomes the member of a single group. The grouping is performed in such a way that a group A sends a merge request to the smallest neighbouring group B. Thus forcing the groups of smaller size to merge, groups of similar size can be merged. If the group B also request to A, then the two groups will merge to form a larger group. If group B reject the group proposal then group A send request to next smallest group. After merging the group A nodes will add a bit zero to the left of their address and group B nodes will add a bit one to left of their address. This will maintain the uniqueness in the address of nodes with in a group. This process of grouping continues until all nodes are under a single group. The nodes can be arranged as the leaves of a binary tree.

Forwarding

The packet is forwarded through multiple paths to achieve high availability of packet delivery. The packet has a source address $R=R_{r-1} \|\ldots\| R_0$ and destination address $R' = R'_{r-1} \|\ldots\| R'_0$. In forwarding the packet the algorithm compares the most significant bits R_{r-1} against R'_{r-1} of both source and destination address. If it is same then the comparison continues to the next most significant bit until it fails for $R_i \neq R'_i$. The routing table entry for position i is verified and the packet is forwarded to the next hop neighbor in that group. Thus the packet will eventually reach the node that match the address digits $R'_{r-1},\ldots,R'_i$.

Disadvantage of secure sensor network routing

In secure sensor network routing, a packet is forwarded in such a way that the packet moves closer to the destination but the algorithm cannot prevent an attacker from rerouting the packet to furthest route. Let as consider the case that an attacker node forward a received packet to a honest node that is more farther away from the destination and that honest node is unable to inform that the packet is moving away from the destination. The node doesn't have the information about previous node address; it has only information about the source and destination address. Thus the attacker will move a packet away from the destination unnoticed. Thus the packet will traverse atmost log N logical hops giving us a theoretical maximum energy increase of O(d),where d is the network diameter and N the number of network nodes [5]. The situation is worse when the packet is routed to attacker itself because again the packet can be rerouted.

C. PLGPa Forwarding Protocol

Y.Vasserman et al introduced PLGPa forwarding protocol as an extension to secure sensor network routing [5]. Here the address creation and routing table creation are done by recursive grouping algorithm as in secure sensor network routing. The forwarding phase of secure sensor network routing is changed to remove the backtracking attack, which is rerouting the packet to largest path.

Packet forwarding

To prevent the backtracking attack (moving the packet away from the destination), a verification path history is added to every packet in the network called attestation field. When a packet is received by a node, it adds its signature to the chain of signature created by the previous nodes. The signature cannot be faked by any malicious nodes since each nodes key is secret. These signatures form a chain attached to every packet, allowing any node receiving it to validate its path. Every forwarding node verifies the attestation chain to ensure that the packet has never travelled away from its destination in the logical address space. The attestation field is created in such a way that the entries in chain cannot be removed or altered. It is a one way chain where signature can only be appended.

When any node receives a message, it checks that every node in the path attestation has a corresponding entry in the signature chain, and is logically closer to the destination than the previous hop in the chain. In this way, forwarding nodes can enforce the forward progress of a message, preserving no backtracking. If no attestation is present, the node verifies that the sender is a physical neighbour and it is the sender of the packet. Since message are signed with the originator's key, malicious nodes cannot falsely claim to be the origin of a message and therefore do not benefit by removing attestation. It any fault in attestation field is found then the packet is rejected.

Advantage of PLGPa

PLGPa algorithm effectively prevents the backtracking attack in secure sensor network routing. The attacker cannot change the attestation field since it follows one way append rule. Thus no one can remove the signature and add new signature. The attacker cannot change the signature since the key is only known by corresponding node. Thus the two phases of the routing protocol, the address and routing table creation phase and the forwarding phase are made secure.

IV. Conclusions

WSN has a large application in the critical and remote areas. WSN provides instant deployable communication and computational power to the users in these areas. The attackers are focusing on the permanent denial of service of the network. Many energy saving and attack preventing protocols and methods are introduced. Some of the methods are discussed and compared in this paper.

An on-demand minimum energy routing protocol reduces the cost of transmission to a larger extent but the attackers are still active in the network. Packet leash is a good method to block attack packets but the cost of synchronization is large and is not economic. The Secure sensor network routing protocol is vulnerable to backtracking attack, thus modification is made to this protocol and PLGPa is created. PLGPa is a better method to protect against the attackers.

REFERENCES

[1] Sheetalkumar Doshi, Shweta Bhandare, and Timothy X. Brown, An on demand minimum energy routing protocol for a wireless ad hoc network, ACM SIGMOBILE Mobile Computing and Communications Review 6 (2002), no. 3.

[2] Yih-Chun Hu, Adrian Perrig and David B. Johnson. Packet leashes: A defense against wormhole attacks in wireless ad hoc networks, INFOCOM, 2003.

[3] Amir Qayyum, Laurent Viennot, and Anis Laouiti. Multipoint Relaying: An Efficient Technique for flooding in Mobile Wireless Networks. Technical Report Research Report RR-3898, INRIA, February 2000.

[4] Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig, Secure sensor network routing: A clean-slate approach, CoNEXT, 2006.

[5] Eugene Y. Vasserman and Nicholas Hopper. Vampire attacks: Draining life from wireless ad-hoc sensor networks. Kansas State University, University of Minnesota.

[6] Charles E. Perkins and Pravin Bhagwat. Highly Dynamic Destination Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. In Proceedings of the SIGCOMM '94 Conference on Communications Architectures, Protocols and Applications, pages 234.244, August 1994.

[7] Bhargav Bellur and Richard G. Ogier. A reliable, efficient topology broadcast protocol for dynamic networks. In Proceedings of the Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies, pages 178.186, March 1999.